IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH DARKNEXTAD@GMAIL.COM THAT IS STORED AT A PREMISES CONTROLLED BY GOOGLE, INC 1600 AMPITHEATRE PARKWAY, MOUTAIN VIEW, CA 94043	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Mandala Fellenz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, Inc., hereinafter referred to as Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

The statements contained in this Affidavit are based in part on information provided by Special Agents of the Federal Bureau of Investigation (FBI) and other law enforcement personnel, information gathered through first-hand investigation, and my experience and

background as a Special Agent with FBI. I have been employed as a Special Agent with the FBI since October 2005. I have gained expertise in the conduct of such investigations through training in the form of seminars, classes, and on the job experience. I have observed and reviewed examples of child pornography, as defined by 18 U.S.C. § 2256, in all forms of media, including computer media. During my assignment with the FBI, I have participated in the execution of numerous search and seizure warrants involving the possession, receipt, and distribution of child pornography and the enticement of minors.

This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252A have been committed by the individual who maintains access and control over the email account DarkNextad@gmail.com. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

PROBABLE CAUSE

By way of background, United States law, Title 18, United States Code §2258A, requires Electronic Service Providers and Internet Service Providers to report any instances that violate federal laws regarding the sexual exploitation of children. This law identifies the National

Center for Missing and Exploited Children (NCMEC) as the central repository for these reports and further permits NCMEC to share this information with law enforcement. The CyberTipline reports are reviewed by NCMEC analysts who forward the information to local law enforcement when they are able to determine the identity and/or location of the subject.

On March 17, 2017, Dropbox notified the CyberTipline Division of NCMEC that they located fifty-four files depicting child pornography located in the Dropbox account created by email address DarkNextad@gmail.com; Screen/User Name: Alan Vardin. Dropbox is a file hosting service operated by Dropbox, Inc. in San Francisco, CA which offers cloud storage, file synchronization, personal cloud and client software. Based on the information received from Dropbox, CyberTipline Report number 18927852 was generated by NCMEC and basic investigative steps were taken in order to locate the user of the reported Dropbox account. On 04/24/2017, an administrative subpoena was served to DropBox requesting information pertaining to email address DarkNextad@gmail.com; Screen/User Name: Alan Vardin. On 05/05/2017, in Dropbox's response pertaining to the User Account of Alan Vardin, they provided Internet Protocol (IP) Address logs, including the date and time that the account was accessed. IP address 63.153.120.234 was utilized to access the account on December 12, 2016 at 07:09:57 UTC and IP address 75.162.110.19 was utilized to access the account on January 2, 2017 at 06:39:30 UTC. In addition to the Dropbox Account, on 04/24/2017, an administrative subpoena was served to Google to provide information pertaining to e-mail address DarkNextad@gmail.com. On 05/17/2017, Google provided a response that included IP Address log information as well the telephone number (406) 565-2531 which is associated with that DarkNextad@gmail.com account. IP login information indicates that IP address

63.153.120.234 was utilized to access the account on December 12, 2016 at 07:09:57 UTC and IP address 75.162.110.19 was utilized to access the account on January 2, 2017 at 06:39:30 UTC.

Based on the information received from Dropbox and Google, an administrative subpoena was issued to Century Link requesting that they provide information pertaining to the Dropbox login IP addresses 75.162.110.19 and 63.153.120.234 for the dates and times provided in the subpoena responses. Century Link responded, providing the subscriber information at the time of logins as being issued to Anakhan Locker, 3308 S. Mockingbird Way, West Valley City, Utah.

In addition to the subpoena to Century Link, an administrative subpoena was served to Verizon Wireless which requested subscriber information pertaining to telephone number (406) 565-2531, associated with the Google Account. Verizon responded providing the subscriber as Stanley Olsen, PO Box 424, Whitehall, Montana.

On 09/27/2017, based on the subscriber information received from Century Link, CyberTip 18927852 was assigned to the Federal Bureau of Investigation, Salt Lake City Division for follow-up investigation. During November 2017, Agents from the Salt Lake City Division interviewed Anakhan Sky Locker (Locker) concerning the Dropbox activity reported in CyberTip 18927852. Locker cooperated during the interview and provided consent to search his electronic devices. Locker adamantly denied any interest in child pornography. A search of Locker's cellular telephone did not locate any evidence of child pornography. In addition, Agents learned that an individual named Cheyenne Patrick Olsen (Olsen) was living at 3308 S. Mockingbird Way, West Valley City, Utah at the time the child pornography was accessed from that address. Locker had not resided at that address, which belonged to his mother, since 2015. He did pay for the internet service as his mother could not afford it. Locker's mother allowed

Rebecca Olsen and her son Cheyenne Olsen, to stay at her home during the time period that child pornography was reported in the Dropbox Account. Locker believes that Cheyenne has since returned to Montana and is likely residing at 401 East 2nd Street, Whitehall, Montana. Locker believes that Olsen's father is Stanley Olsen.

Following the interview with Locker and based on the identification of Olsen as a possible subject, the investigation was forwarded to the Helena, Montana Resident Agency of the FBI for follow-up investigation. Upon receipt of the information, I reviewed the 54 files provided by Dropbox which were located in the Dropbox Account of User Name Alan Vardin with associated email account of DarkNextad@gmail.com . The 54 files were all video files, the majority of which contained child pornography.

Listed below are a few descriptions of the child pornography video files that I examined:

a. [MB]_-_Dads_Touching_His_Small_Boys_Dick.avi -The file is a video that is approximately 20 seconds in length. It depicts a nude adult male sitting in front of a computer. There is a nude minor male child, who appears to be less than 10 years-old, leaning against the adult male who is seated. The adult male has his arms wrapped around the minor child and is using his hand to manipulate the minor child's penis. The adult male is also pressing the child against him in such a way that the adult male's genital area appears to be rubbing against the minor child's buttocks.

b. 9a9ba575-defe-48f9-ac64-451ae72c80d9.mp4 – The file is a video file approximately 51 seconds in length. It initially depicts a nude prepubescent female wearing what appears to be knee highs. She is performing fellatio on the penis of a dog. The last 5 seconds of the video shows a nude prepubescent female lying flat on her back. Her vaginal area is being manipulated by the hand of an adult male.

c. 518d0e39-eb60-4c6d-bdfb-ec2b27743378.mp4 – The file is a video file that is approximately 32 seconds in length. The file depicts a nude prepubescent female lying on her back. The focus of the video is on her genital area. There is an adult male penis penetrating her vagina. The male's dark colored clothing, penis, and his hand are all that are visible during the video. At approximately 23 seconds into the video, the male removes his penis from her vaginal area and ejaculates on her stomach. The minor female rubs the fluid on her vaginal area.

Additionally, I reviewed the Facebook Page belonging to Olsen. Olsen's Facebook Page appeared after typing in the vanity name of "DarkNextad" into the Facebook Search Tool. An administrative subpoena was issued to Facebook requesting subscriber information for the "DarkNextad" account. On 12/21/2017, Facebook responded providing the subscriber name as Patrick Olsen and an associated telephone number of (406) 565-2531. This number is consistent with the number associated to the DarkNextad@gmail.com account.

Another subpoena was served to Google for the e-mail account of DarkNextad@gmail.com. On 12/19/2017, Google responded and provided subscriber information and IP logins. The telephone number (406) 565-2531 was still associated with the DarkNextad@gmail.com e-mail account and the last login occurred on 12/17/2017 at 07:30 UTC from IP 63.153.106.133, indicating that the account is still being actively used. This IP address belongs to Century Link and therefore an administrative subpoena was served requesting subscriber information regarding that IP address. On 01/19/2018, Century Link responded with the subscriber as being Stanley Olsen, 401 East 2nd Street, Whitehall, Montana.

On 06/15/2017, 09/06/2017, and on 12/05/2017, preservation letters were sent to Google requesting that they preserve the account contents of DarkNextad@gmail.com. In general, an

email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

An Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain

records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

This application seeks a warrant to search all responsive records and information under the control of Google a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [1]

As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or

---

[1] It is possible that Google, Inc. stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Google, Inc. The government also seeks the disclosure of the physical location or locations where the information is stored.

alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

On March 7, 2018, reference Case Number MJ-18-13-M-JCL, I obtained a search warrant for the Google Gmail Account of DarkNextad@gmail.com. After service of the search

warrant, I caught an error on the face of the search warrant in that it didn't reference the attachments so I'm seeking a corrected search warrant.

CONCLUSION

Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Mandala M. Fellenz
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on April 5, 2018

Honorable Jeremiah C. Lynch
UNITED STATES MAGISTRATE JUDGE